Fundamental Theorem of Arithmetic
Two Proofs

Steve Ziskind

1 Statement of Theorem

This very important result says the any integer larger than 1 can only be written as a product of primes in one way, except for trivial rearrangements of the factors. More formally, it says that if $n > 1$ then we can uniquely write

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

where

$$p_1 < p_2 < \cdots < p_k$$

are all primes. Uniqueness is the point of the theorem.

2 First Proof

We first need a lemma based on the Euclidean Algorithm. Recall that a byproduct of the algorithm says that the greatest common divisor of two numbers can be realized as a linear combination of them. Explicitly, given integers a and b, there will exist others integers, x and y, such that
$gcd(a, b) = xa + yb$. We take this as known.

Lemma: If p is prime, $p \mid ab$, but $p \nmid a$, then $p \mid b$.

Proof: Because p is prime, its only divisors are 1 and p. But if $p \nmid a$ then gcd(p,a) = 1. By the Euclidean Algorithm there are integers x and y for which $1 = xp+ya$. Multiplying both sides by b we find that $b = abp+yab$. But $p \mid ab$, so $ab = zp$ for some z. Inserting this into the prior equation we have $b = abp + yzp = p(ab + yz)$, expressing b as a multiple of p, as asserted. QED

Using induction, the lemma says that if a prime divides a product, perhaps with many factors, then it must divide one or more of the factors.

Proof of Theorem: We can check directly that the smallest numbers, such 2, 3, etc can only factor one way. If there were a number with two distinct prime factorizations, then there would be a smallest such. Selecting one of the primes from the first product, the lemma says that it will divide one of the factors from the second product. Cancelling this prime from both, we get a smaller number with multiple factorizations, contradicting the original choice of the smallest such. QED

3 Second Proof

Suppose that n is the smallest number that can be factored into primes in several ways. Write

$$n = p_1 p_2 p_3 \cdots = q_1 q_2 q_3 \ldots$$

If any of the p and q factors were the same it could be cancelled from both sides, giving a smaller number with several factorizations. Thus $p_1 \neq q_1$. One of them must be larger, so suppose $p_1 > q_1$. Now define the number

$$m = (p_1 - q_1) p_2 p_3 \cdots = q_1 (q_2 q_3 \cdots - p_2 p_3 \ldots)$$

Clearly q_1 divides the second product, but divides none of the factors of the first product. So now m has two distinct product representations, but is smaller than n, contradicting the choice of n as the smallest number with two representations. QED